UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/762,555	04/10/2001	Lothrop Mittenthal	TET-1668/980	6718

7590 11/10/2003

Robert A Muha
Kirkpatrick & Lockhart
Henry W Oliver Building
535 Smithfield Street
Pittsburgh, PA 15222-2312

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 11/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/762,555	MITTENTHAL, LOTHROP
	Examiner	Art Unit
	Christian La Forgia	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 April 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. The amendment filed on 16 August 2001 is noted and made of record.

2. Claims 1 through 22 are presented for examination.

Drawings

3. The informal drawings filed in this application are acceptable for examination purposes.

When the application is allowed, applicant will be required to submit new formal drawings.

4. The Patent and Trademark Office no longer makes drawing changes. See 1017 O.G. 4.

It is applicant's responsibility to ensure that the drawings are corrected. Corrections must be made in accordance with the instructions below.

INFORMATION ON HOW TO EFFECT DRAWING CHANGES

Replacement Drawing Sheets

Drawing changes must be made by presenting replacement figures which incorporate the desired changes and which comply with 37 CFR 1.84. An explanation of the changes made must be presented either in the drawing amendments, or remarks, section of the amendment. Any replacement drawing sheet must be identified in the top margin as "Replacement Sheet" and include all of the figures appearing on the immediate prior version of the sheet, even though only one figure may be amended. The figure or figure number of the amended drawing(s) must not be labeled as "amended." If the changes to the drawing figure(s) are not accepted by the examiner, applicant will be notified of any required corrective action in the next Office action. No further drawing submission will be required, unless applicant is notified.

Identifying indicia, if provided, should include the title of the invention, inventor's name, and application number, or docket number (if any) if an application number has not been assigned to the application. If this information is provided, it must be placed on the front of each sheet and centered within the top margin.

Annotated Drawing Sheets

A marked-up copy of any amended drawing figure, including annotations indicating the changes made, may be submitted or required by the examiner. The annotated drawing sheets must be clearly labeled as "Annotated Marked-up Drawings" and accompany the replacement sheets.

Timing of Corrections

Applicant is required to submit acceptable corrected drawings within the time period set in the Office action. See 37 CFR 1.85(a). Failure to take corrective action within the set period will result in ABANDONMENT of the application.

If corrected drawings are required in a Notice of Allowability (PTOL-37), the new drawings MUST be filed within the THREE MONTH shortened statutory period set for reply in the "Notice of Allowability." Extensions of time may NOT be obtained under the provisions of 37 CFR 1.136 for filing the corrected drawings after the mailing of a Notice of Allowability.

Specification

5. This application does not contain an abstract of the disclosure as required by 37 CFR 1.72(b). An abstract on a separate sheet is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "maximal" in claims 1 through 22 is used by the claim to mean "a function that can be applied recursively to generate the entire orthomorphic mapping", while the accepted meaning is "an element in an ordered set that is followed by no other." The term is indefinite because the specification does not clearly redefine the term.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1 through 22 are rejected under 35 U.S.C. 102(a) based upon a public knowledge of the invention. Chapter 2132 of the MPEP states:

> The statutory language known or used by others in this country' (35 U.S.C. § 102(a)), means knowledge or use which is accessible to the public.

The instant invention was available to the public in this country as early as March 1995, as published in **Advances in Applied Mathematics**, vol. 16, No. 1. The various claim limitations of the independent claims are drawn to various parts of the article, both explicitly and inherently. As per the first two limitations, the two generating functions, they are inherent to the system as defined by the inventor. Proof of this lies in **Applied Cryptography: Protocols, Algorithms, and Source Code in C**, by Bruce Schneier on page 347, which states:

> Most block algorithms are Feistel networks. This idea dates from the early 1970s. Take a block of length *n* and divide it into two halves of length n/2: *L* and *R*. Of course, *n* must be even. You can define an iterated block cipher where the output of the *i*th round is determined from the output of the previous round...

Therefore, it is inherent to most block algorithms to provide for a first and second generating function. See MPEP § 2132. The selecting of a first and second set of linearly independent

numbers is disclosed on page 61 of **Block Substitutions Using Orthomorphic Mappings**, by Lothrop Mittenthal, in which the article states:

> The next step is to select a candidate for x_{n+1} such that {x2, x3,..., xn+1} and {z2, z3,...,zn+1} are each linearly independent sets.

Therefore, Mittenthal teaches the selecting of a first and second set of linearly independent numbers. The last two claim limitations are commonly drawn to pages 63 through 65 of the Mittenthal paper. See also *Carella v. Starlight Archery,* 804 F.2d 135, 231 USPQ 644 (Fed. Cir. 1986).

10. Claims 16 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 6,182,216 to Luyster, hereinafter Luyster.

11. As per claim 16, Luyster teaches a computer-implemented method for deterministically generating maximal nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

selecting a second set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

generating plurality of linear orthomorphisms using first and second recursive generating function and the first and second sets of linearly independent numbers (Figure 1 [blocks 16, 18],

3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60); and

setting the maximal nonlinear substitution tables based on a combination of the linear orthomorphisms, the substitution tables for use in encrypting clear text messages which are in the form of a sequence of bin numbers (Figure 1 [block 44], 3 [block 88], 6 [block 148], 7 [block 188], 9 [block 230], 14 [block 346]; column 21, lines 25-60; column 43, lines 16-22; column 45, lines 8-16).

12. As per claim 18, Luyster teaches a computer implemented method for deterministically generating maximal nonlinear block substitution tables from binary data, comprising:

selecting a first set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

selecting a second set of a plurality of complete linearly independent numbers from the binary data (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

recursively applying a first generating function to the first set of linearly independent numbers to create a major cycle o a first orthomorphism (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60);

generating a plurality of cycles of the first orthomorphism (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60);

recursively applying a second generating function to the second set of linearly independent numbers to create a major cycle of a second orthomorphism; generating a plurality of cycles of the second orthomorphism (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60); and

setting the maximal nonlinear substitution tables by combining the linear orthomorphisms, the substitution tables for us in encrypting clear text messages which are in the form of an ordering of binary numbers (Figure 1 [block 44], 3 [block 88], 6 [block 148], 7 [block 188], 9 [block 230], 14 [block 346]; column 21, lines 25-60; column 43, lines 16-22; column 45, lines 8-16).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1 through 15, 17, and 19 through 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Luyster in lieu of obviousness.

15. As per claim 1, Luyster teaches method of deterministically generating maximal nonlinear block substitution tables for a predetermined block size, comprising:

selecting a first generating function (Figures 1 [blocks k1, k2], 2 [block key1, key 2], 5 [blocks 92, 100g], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting a second generating function (Figures 5 [blocks 94, 100h], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting first and second sets of complete linearly independent numbers (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60); and

creating maximal nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages (Figure 1 [block 44], 3 [block 88], 6 [block 148], 7 [block 188], 9 [block 230], 14 [block 346]; column 21, lines 25-60; column 43, lines 16-22; column 45, lines 8-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to split up the generating function of Luyster into two separate generating functions. As it is commonly recognized by those of ordinary skill in the art, block ciphers split the blocks in half according to bit size, i.e. a 32 bit block will be split into two 16 bit halves, a 64 bit block will be split into two 32 bit halves, and so on and so forth. Likewise, it is commonly recognized that these generated keys will be combined with the plain text to create the cipher text. Therefore the separating of the generating

functions of Luyster would be obvious because it is merely shifting the location of the parts. See MPEP § 2144.04. See also *In re Japikse*, 181 F.2d 1019, 1023, 86 USPQ 70, 73 (CCPA 1950).

16. Regarding claim 2, Luyster teaches wherein selecting a first generating function includes selecting a first primitive generating function (Figure 6; column 37, lines 55 to column 38, lines 23). Luyster teaches the generating functions comprising such primitive functions as addition, subtraction, and division.

17. Regarding claim 3, Luyster teaches wherein selecting a first generating function includes selecting a first nonprimitive generating function (Figure 6; column 37, lines 28-45). Luyster teaches the generating functions being performed recursively, wherein the keys being generated are dependent on the data in the previous round.

18. Regarding claim 4, Luyster teaches wherein selecting a second generating function includes selecting a second primitive generating function (Figure 6; column 37, lines 55 to column 38, lines 23). Luyster teaches the generating functions comprising such primitive functions as addition, subtraction, and division.

19. Regarding claim 5, Luyster teaches wherein selecting a second generating function includes selecting a second nonprimitive generating function (Figure 6; column 37, lines 28-45). Luyster teaches the generating functions being performed recursively, wherein the keys being generated are dependent on the data in the previous round.

20. With regards to claim 6, Luyster teaches wherein selecting a second non-primitive generating function includes selecting a second non-primitive generating function having a cycle pattern that is identical to a cycle pattern of the first generating function (column 37, lines 18-45).

21. Regarding claim 7, Luyster teaches wherein calculating first and second linear orthomorphisms includes calculating first and second maximal linear orthomorphisms from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60).

22. Regarding claim 8, Luyster teaches further comprising rotating the second linear orthomorphism (column 37, lines 37-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to rotate the second linear orthomorphism. One would be motivated to adopt this technique because it is fast, simple, and add more security.

23. With regards to claim 9, Luyster teaches wherein rotating the second linear orthomorphism includes rotating corresponding cycles of the second linear orthomorphism (column 37, lines 37-45).

24. Regarding claim 10, Luyster teaches wherein selecting a second generating function includes selecting a second generating function which is a complement of the first generating function (column 38, lines 5-36; column 39, line 60 to column 40, lines 28).

25. Regarding claim 11, Luyster teaches wherein selecting a second generating function includes selecting a second generating function which is any generating function that is not identical to the first generating function and has a cycle structure which matches a cycle structure of the first generating function (column 38, lines 5-36; column 39, line 60 to column 40, lines 28).

26. Regarding claim 12, Luyster teaches wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is identical to the first set of linearly independent numbers (column 39, lines 17-28).

27. Regarding claim 13, Luyster teaches wherein selecting first and second sets of linearly independent numbers includes selecting a second set of linearly independent numbers that is not identical to the first set of linearly independent numbers (column 39, lines 17-28).

28. Regarding claim 14, Luyster teaches further comprising determining whether all cycles of the first and second linear orthomorphisms are self-contained (column 23, line 50 to column 24, line 27).

29. With regards to claim 15, Luyster teaches further comprising selecting pairs of cycles from the first and second linear orthomorphisms to produce a mapping for which N(x,y)!=0 for all pairs of numbers from different cycles (Figure 12; column 33, line 37 to column 34, line 36).

30. Regarding claims 17 and 19, Luyster teaches wherein the second generating function is a complement of the first generating function (column 39, lines 17-28). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the second function be a complement of the first function. It merely be a fact of reversing parts to ensure different keys between the two halves. See MPEP § 2144.04. See also *In re Gazda*, 219 F.2d 449, 452, 104 USPQ 400, 402 (CCPA 1955).

31. As per claims 20, 21 and 22, Luyster teaches a system, comprising:

a communications link (column 56, line 60 to column 57, line 12);

a first computer in communication with the communications link (column 56, line 60 to column 57, line 12); and

a second computer in communications with the communications link (column 56, line 60 to column 57, line 12), the second computer having an ordered read set of data and instructions stored thereon which, when executed by the second computer cause the second computer to perform the steps of:

selecting a first generating function (Figures 1 [blocks k1, k2], 2 [block key1, key 2], 5 [blocks 92, 100g], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting a second generating function (Figures 5 [blocks 94, 100h], 11; column 38, lines 24-36; column 51, lines 19-67);

selecting first and second sets of complete linearly independent numbers (Figures 1 [blocks 12, 14], 2 [blocks 16, 18], 3 [blocks 52, 54], 4 [blocks 52, 56], 6 [blocks 112, 114], 7 [blocks 152, 154], 8 [block 152, 154], 9 [blocks 192, 194], 14 [blocks 302, 304]; column 11, lines 42-49; column 18, lines 54-67; column 42, lines 22-28);

calculating first and second linear orthomorphisms from the generating functions and the sets of linearly independent numbers (Figure 1 [blocks 16, 18], 3 [blocks 84, 86], 6 [blocks 144, 146], 7 [blocks 184, 186], 9 [block 226, 228], 14 [blocks 342, 344]; column 22, lines 6-25; column 42, lines 28-38; column 57, lines 20-60); and

creating maximal nonlinear block substitution tables by combining the linear orthomorphisms, the block substitution tables for use in encrypting clear text messages (Figure 1 [block 44], 3 [block 88], 6 [block 148], 7 [block 188], 9 [block 230], 14 [block 346]; column 21, lines 25-60; column 43, lines 16-22; column 45, lines 8-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to split up the generating function of Luyster into two separate generating functions. As it is commonly recognized by those of ordinary skill in the art, block ciphers split the blocks in half according to bit size, i.e. a 32 bit block will be split into two 16 bit halves, a 64 bit block will be split into two 32 bit halves, and so on and so forth. Likewise, it is commonly recognized that these generated keys will be combined with the plain text to create the cipher text. Therefore the separating of the generating functions of Luyster would be obvious because it is merely shifting the location of the parts. See MPEP § 2144.04. See also *In re Japikse*, 181 F.2d 1019, 1023, 86 USPQ 70, 73 (CCPA 1950).

Double Patenting

32. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

33. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

34. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

35. Claims 1 through 22 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 through 34 of U.S. Patent No. 6,035,042. Although the conflicting claims are not identical, they are not patentably distinct from each other because there are significant similarities amongst the claim language. For instance, claim 1 of the patent discusses selecting a first and second set of distinct output numbers, combining the two sets of data, and creating a substitution table to encrypt a plain text, steps (a), (b), (c), and (g), respectively. These steps are drawn to the last three limitations of the

independent claims disclosed in the instant application. It is further asserted above that the two generating functions are inherent to most block algorithms, and therefore inherent to U.S. Patent No. 6,035,042.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

37. The following patents are cited to further show the state of the art with respect to block ciphers, such as:

United States Patent No. 5,724,428 to Rivest, which is cited to show a block encryption algorithm with data-dependent rotations.

United States Patent No. 5,835,600 to Rivest, which is cited to show a block encryption algorithm with data-dependent rotations.

United States Patent No. 5,054,067 to Moroney et al., which is cited to show a block cipher cryptographic device.

United States Patent No. 6,249,582 to Gilley, which is cited to show how to reduce overhead in a block cipher.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

39. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

40. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Christian La Forgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100